MICHELANGELO *Office PRO V*

Modem/Router ADSL con Switch 4 porte e VLAN

Manuale Operativo

rev. 1.0 del 10/2005

INDICE

DICHIARAZIONE CE DI CONFORMITA'

Noi, **Digicom S.p.A. via Volta 39 - 21010 Cardano al Campo (Varese - Italy)** dichiariamo sotto la nostra esclusiva responsabilità, che i prodotti, Nome: **MICHELANGELO Office Pro V** al quale questa dichiarazione si riferisce, soddisfano i requisiti essenziali della sotto indicata Direttiva:

- **1999/5/CE** del 9 marzo 1999, R&TTE, (riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità).
  Come designato in conformità alle richieste dei seguenti Standard di Riferimento o ad altri documenti normativi:
  - EN 55022
  - EN 61000-3-2
  - EN 61000-3-3
  - EN 301 489-1
  - EN 301 489-17
  - ITU-T K.21
  - EN 60950

PREMESSA

Al fine di salvaguardare la sicurezza, l'incolumità dell'operatore ed il funzionamento dell'apparato, devono essere rispettate le seguenti norme installative:

CONDIZIONI AMBIENTALI

Temperatura ambiente	Umidità relativa
da 0 a +40°C	dal 20 a 90% n.c.

Si dovrà evitare ogni cambiamento rapido di temperatura e umidità

- Polvere, umidità, calore elevato ed esposizione diretta alla luce del sole.
- Oggetti che irradiano calore. Questi potrebbero causare danni al contenitore o altri problemi.
- Oggetti che producono un forte campo elettromagnetico (altoparlanti Hi-Fi, ecc.)
- Liquidi o sostanze chimiche corrosive.

AVVERTENZE GENERALI

Per evitare scosse elettriche, non aprite l'apparecchio o il trasformatore. Rivolgetevi solo a personale qualificato.
Scollegate il cavo di alimentazione dalla presa a muro quando non intendete usare l'apparecchio per un lungo periodo di tempo.
Per scollegare il cavo tiratelo afferrandolo per la spina. Non tirate mai il cavo stesso.
In caso di penetrazione di oggetti o liquidi all'interno dell'apparecchio, scollegate il cavo di alimentazione e fate controllare da personale qualificato prima di utilizzarlo nuovamente.

PULIZIA DELL'APPARATO

Usare un panno soffice asciutto senza l'ausilio di solventi.

VIBRAZIONI O URTI

Attenzione a non causare vibrazioni o urti.

Smaltimento delle apparecchiature obsolete

Tutti i prodotti elettrici ed elettronici, devono essere smaltiti separatamente rispetto alla raccolta differenziata municipale, mediante impianti di raccolta specifici designati dal governo o dalle autorità locali.
Quando sul prodotto è riportato il simbolo di un bidone della spazzatura barrato da una croce, significa che l'apparato è coperto dalla direttiva europea 2002/96/EC (WEEE).
Sono previste sanzioni, in caso di smaltimento abusivo di detti prodotti.

1. INTRODUZIONE

Gentile Cliente,
la ringraziamo per la fiducia accordataci nell'acquistare un prodotto Digicom.

Michelangelo Office Pro V riunisce in un unico dispositivo tutte le funzionalità e le caratteristiche necessarie a realizzare un efficiente accesso ad Internet via ADSL, fornendo nel contempo la protezione della rete LAN locale da attacchi provenienti dal mondo esterno, tramite un firewall integrato.

Il supporto VPN (Virtual Private Network) offre la possibilità di fornire l'accesso alla rete LAN locale anche ad utenti remoti (client o LAN) in modo sicuro e protetto da crittografia dei dati.

La gestione del QoS e delle Virtual Lan permettono di raggiungere un ottimo livello di ottimizzazione del traffico sulla LAN.

Prerequisiti

- Computer con schede di rete Ethernet 10/100 Mbps
- Protocollo TCP/IP installato su ogni macchina
- Cavi di rete dritti, connettori RJ45 su entrambe le estremità
- Linea ADSL su linea analogica, connettore RJ11
- Abbonamento ADSL singolo utente o multiutente stipulato con un ISP
- Dati relativi all'abbonamento

Contenuto della confezione

- 1 Michelangelo Office Pro V
- 1 Alimentatore
- 1 CD-ROM completo di manuali
- Manuale di configurazione rapida
- 1 cavo RJ45-RJ45 dritto
- 1 cavo di linea RJ11-RJ11

1.1. CARATTERISTICHE

ADSL, ADSL2, ADSL2+

- Velocità dati asimmetrica
- Velocità massima Ricezione (downstream) : 24Mbit/s(ADSL2+), 12Mbit/s(ADSL2), 8Mbps(ADSL)
- Velocità massima Trasmissione (upstream) : 1Mbit/s
- Standard ADSL:
  ANSI T1.413, Issue 2;
  G.dmt (ITU G.992.1);
  G.lite (ITU G.992.2);
  G.hs (ITU G994.1);
  G.dmt.bis (ITU G.992.3);
  G.dmt.bisplus (ITU G.992.5)
- Protocolli Supportati :
  RFC 2364 (PPP over ATM)
  RFC 2516 (PPP over Ethernet)
  RFC 1483 (Bridged e Routed Ethernet over ATM)
- Interfaccia WAN ADSL: Connettore RJ11

LAN

- Switch 4 porte 10/100 Mbit/s
- Funzione MDI / MDI-X su tutte le 4 porte
- Supporto IP Alias
- DHCP Server e Relay
- Supporto VLAN
- Ethernet Client Filter

FIREWALL

- Protocollo NAT
- Protezione Packet Filter
- Protezione MAC Address Filter
- Protezione URL Filter
- Intrusion Detection (Protezione da attacchi tipici, Denial of Service e Scan)

APPLICAZIONI AVANZATE

- Client e Server VPN con protocollo PPTP e IPSEC, L2TP
- QoS – Quality of Service Lan -> Wan, Wan -> Lan
- Esportazione servizi (Virtual Server)
- Supporto DMZ
- Dynamic DNS
- Check Emails

1.2. DESCRIZIONE PORTE E LED

Fig. 1.1. Vista frontale

PWR	Acceso quando il router è alimentato
SYS	Acceso quando il sistema è pronto
LAN Port 1-4	Accese quando un dispositivo Ethernet è collegato alla relativa porta LAN Verde -> connesso a 100Mbit/s Arancione -> connesso a 10Mbit/s Lampeggiante indica l'attività dati sulla porta LAN
PPP/MAIL	Acceso quando è attiva una connessione ADSL di tipo PPPoA oppure PPPoE Lampeggiante periodicamente se sono stati rilevati nuovi messaggi e-mail dalla funzione Check Emails
ADSL	Acceso indica che la connessione ADSL è stabilita

Fig. 1.2. Vista posteriore

LINE	Ingresso per la linea ADSL, connettore RJ-11
Console	Porta di console PS2/RS-232 per l'accesso alla configurazione
LAN 1-4	Porta LAN per collegare dispositivi Ethernet, connettori RJ-45
Reset	Tasto di reset. Tenendo premuto il tasto di reset per n secondi si effettuano le seguenti operazioni: 0-3 secondi -> reset software (off/on del Router) più di 6 secondi -> reset hardware, ripristino alle impostazioni di fabbrica
PWR	Ingresso per l'alimentatore
Power Switch	Interruttore di accensione, Power ON - Power OFF

2. INSTALLAZIONE

Alimentazione

Alimentate il Router utilizzando l'alimentatore fornito nella confezione quindi accendete il dispositivo tramite l'apposito interrurrore di accensione **Power Switch**.

Connessione ADSL

Collegate la linea ADSL al connettore **LINE** presente nel pannello posteriore.

Connessione LAN

Collegate i Computer della vostra LAN (fino a quattro) direttamente al Router ad una delle porte LAN presenti nel pannello posteriore.

Se disponete di una rete LAN pre-esistente, collegate una delle porte LAN del router ad una porta del vostro HUB o Switch di rete LAN, tramite un cavo RJ45-RJ45 diritto (funzionalità MDI/MDI-X automatica effettuata dal router).

3. CONFIGURAZIONE

Per effettuare la configurazione del Router è necessario disporre di tutti i dati relativi al Vostro abbonamento ADSL. Questi dati vi devono essere forniti dal provider Internet con il quale avete stipulato il contratto di accesso ad Internet su ADSL.

I parametri richiesti solitamente sono:

- VPI / VCI (normalmente 8 / 35)
- Tipo di protocollo (PPP over ATM, PPP over Ethernet, RFC 1483…..)
- Indirizzi IP dei DNS utilizzati dal provider
- Username e Password oppure IP assegnati.

3.1. CONFIGURAZIONE DEL COMPUTER

Per accedere alla configurazione del router è indispensabile che il computer utilizzi il protocollo TCP/IP e che disponga di un comune Browser grafico (Explorer, Netscape, Opera …).
Le impostazioni di fabbrica (default) del router sono:

Indirizzo IP: 192.168.1.254
Subnet Mask: 255.255.255.0
DHCP Server: Abilitato

Per accedere alla configurazione quindi occorre impostare sul computer un indirizzo IP della stessa rete del router; potete impostare l'indirizzo in modo statico oppure utilizzare l'assegnamento con DHCP Server.

Windows® XP
Dal menù **Start** selezionate -> **Pannello di Controllo** -> **Rete e Connessioni Internet** , **Risorse di rete** e selezionate **Visualizza risorse di rete**.
Selezionate **Connessione alla rete locale** (**LAN**) e visualizzate le Proprietà, selezionate **Protocollo Internet** (**TCP/IP**) e premete sul pulsante **Proprietà**.
Se volete utilizzare un indirizzo IP Statico inserite un indirizzo 192.168.1.x (con x compreso tra 1 e 253), Subnet Mask 255.255.255.0 e gateway 192.168.1.254
Se volete utilizzare un DHCP Server, impostate "**ottieni automaticamente un indirizzo IP**".

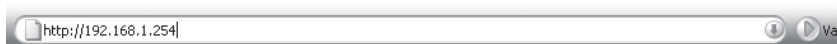
3.2. CONFIGURAZIONE MICHELANGELO OFFICE PRO V

3.2.1. REGOLE GENERALI DI CONFIGURAZIONE

1. Il PC dal quale eseguite la configurazione del Router deve essere privo di software proxy o firewall. Se utilizzate dei programmi di proxy, firewall o similari, disattivateli temporaneamente per poter effettuare la configurazione del Router.
2. In ogni finestra di configurazione premete **Apply** per attivare le impostazioni; le modifiche hanno effetto immediato.
3. Per **salvare** le impostazioni in modo definitivo (in modo che rimangano attive anche dopo uno spegnimento del router) selezionate l'opzione **Save Config to FLASH** e successivamente **Apply**

3.2.2. ACCESSO ALLA CONFIGURAZIONE DEL ROUTER

Aprite il vostro Browser e verificate che non sia impostato per utilizzare un proxy.

Digitate l'URL **http://192.168.1.254**
Nota: 192.168.1.254 è l'indirizzo IP di fabbrica del router

Vi verrà richiesto di autenticarvi per poter accedere alla configurazione del Router:

Inserite:

Nome utente: admin
Password: admin

Nota: admin è la username e password di fabbrica del router. Vi consigliamo di modificarle successivamente, una volta terminata la configurazione, per motivi di sicurezza.

Selezionate la voce **Configuration** per configurare tutte le funzionalità del dispositivo.

3.3. CONFIGURATION – LAN

3.3.1. BRIDGE INTERFACE

Grazie alle funzionalità di VLAN è possibile effettuare una divisione logica della rete aziendale in 4 diversi gruppi.

P1-P4: rappresentano le porte fisiche di LAN, dalla 1 alla 4
Ethernet-Ethernet3: rappresentano i gruppi logici creati tra le porte

Nell'immagine precedente sono stati creati 2 gruppi, Ethernet che include le porte 1 e 2, Ethernet1 che include le porte 3 e 4. Cliccando sul nome di un gruppo si accede alla configurazione del gruppo.

3.3.2. ETHERNET

Michelangelo Office Pro-V Adsl 2+ è in grado di gestire più indirizzi IP di LAN.
Utilizzando questa funzionalità è possibile fornire accesso ad Internet a 2 reti distinte allo stesso tempo.
Il campo **Primary IP Address** rappresenta l'indirizzo IP principale del dispositivo, impostate qui l'indirizzo che volete utilizzare.
Per aggiungere un ulteriore indirizzo IP selezionate il tasto **Add** nella sezione **IP Alias.**

Abilitate, se necessario l'invio e ricezione di pacchetti **RIP** versione 1, 2 ed il supporto Multicast.
Selezionate **Apply** per attivare le impostazioni effettuate.

Nota: l'indirizzo IP diventerà attivo da subito, se cambiate classe di indirizzo IP per completare la configurazione è necessario modificare l'indirizzo IP del Pc e successivamente rientrare in configurazione.

3.3.3. ETHERNET CLIENT FILTER

Questa funzionalità permette di abilitare o disabilitare l'accesso ad Internet ad un elenco di host (max. 16) basandosi sull'indirizzo fisico (MAC Address) della scheda.

Ethernet Client Filter: abilita la funzionalità MAC Address Filter

Allowed: Il router è abilitato ad operare **solamente** con i MAC address inseriti nella tabella, tutte le altre schede di rete non possono comunicare con e attraverso il router.

Blocked: Il router comunica con tutte le macchine, **ad esclusione** di quelle con il MAC address inserito in tabella.

MAC Address: Inserite gli indirizzi MAC

Cliccando sul link *Candidates* è possibile visionare tutti i Mac Address dei dispositivi attualmente collegati al router, per permetterne un rapido inserimento.

3.3.4. PORT SETTING

Questo menu permette di impostare i parametri di funzionamento delle porte LAN.

Port (1-4) Connection Type: Ogni porta Ethernet può essere singolarmente configurata per operare in automatico, velocità fissa 10 o 100Mbit, Half o Full duplex. Utilizzare l'impostazione 'auto' a meno che non si debba forzare la velocità o modalità di funzionamento per apparati non in grado di negoziarla correttamente.

IPv4 TOS priority Control: Abilita il controllo del byte di TOS e delle priorità in esso impostate nel pacchetto IP.

3.3.5. DHCP SERVER

Questo menu permette di impostare i parametri relativi al servizio DHCP:

DHCP Server Mode

- Disable: Disabilita il DHCP Server.
- DHCP Server : Abilita il DHCP Server interno del router.
- DHCP relay agent: permette l'utilizzo di Server DHCP già presenti in rete. Le richieste DHCP che perverranno al router verranno reindirizzate al DHCP di rete impostato.

Selezionando NEXT è possibile modificare le impostazioni del server DHCP.

Il DHCP Server può essere attivato solamente sul **Primary IP Address.**

Allow Bootp: se abilitato assegna l'indirizzo IP anche ai client che utilizzano il bootp

Allow Unknown Client: se abilitato assegna un indirizzo IP a tutti i client che ne fanno richiesta.
Se disabilitato solo i client inseriti in ***Fixed Host*** potranno ricevere un indirizzo IP.

Use Default Range: imposta automaticamente il range utilizzando i primi 20 indirizzi della rete.

Starting-Ending IP Address: definiscono un range di indirizzi IP (inizio – fine) che il DHCP server può allocare ai vari client.

Lease Time: imposta il tempo di default e il tempo massimo di validità di un indirizzo IP, una volta assegnato tramite DHCP server. Non modificate questi valori se non avete esigenze particolari.

Use Router as DNS Server: assegna l'indirizzo IP del router come server DNS.
Il Router dovrà avere impostati gli indirizzi DNS nella apposita finestra di configurazione della sezione WAN per poter operare come DNS Proxy.

Primary / Secondary DNS Server Address: Se il DHCP server deve assegnare degli indirizzi di DNS prefissati, inseriteli in questi campi e disabilitate la funzione "Use Router as DNS Server Address".

Use Router as Default Gateway: assegna l'indirizzo IP del router come Gateway.
Disabilitate questa funzione solamente se volete fornire accesso alla rete LAN ai client DHCP senza permettere loro la navigazione.

E' possibile assegnare sempre lo stesso indirizzo IP ad una determinata macchina, creando degli IP riservati, tramite il menu **FixedHost**.

Name: Inserite un nome mnemonico per la macchina
IP Address: Inserite l’indirizzo IP che volete assegnare alla macchina.
MAC Address: Inserite l’indirizzo MAC della scheda di rete che identifica la macchina.
Maximum Lease Time: Tempo di validità dell’indirizzo IP assegnato.

Una volta creato un FixedHost è possibile visualizzare l’elenco degli host configurati:

Edit: permette la modifica dell’Host
Delete: cancella l’Host
Create: visualizza la finestra ‘FixedHost Create’ per aggiungere un nuovo Host.

DCHP Relay Agent

Impostando questa modalità se il router riceve una richiesta di indirizzo IP tramite Dhcp la inoltra ad un server Dhcp già presente in rete.

DHCP Server IP Address: Impostate l’indirizzo IP del server DHCP già presente in rete

Cliccate sul tasto **Apply** per attivare questa configurazione.

3.4. CONFIGURATION – WAN

In questo menu è possibile inserire i parametri di accesso alla linea ADSL.

3.4.1. ISP

Nella sezione **ISP** (Interner Service Provider) selezionare il tipo di protocollo utilizzato dalla linea Adsl .

3.4.2. LINEA PPPOA / PPPOE

Le linee con indirizzo IP dinamico utilizzano il protocollo PPPoA, oppure il protocollo PPPoE (quest'ultimo generalmente solo su richiesta). Questo tipo di linee prevedono un autenticazione tramite un nome utente ed una password.

Selezionate **PPPoA router** se disponete di questo tipo di linea, selezionate **Next:**

VPI e **VCI:** se non diversamente indicati nel contratto di attivazione della linea Adsl, inserite rispettivamente **8** e **35** come nell'esempio.

ATM Class: Lasciate impostato UBR; impostate un altro valore solo se espressamente richiesto dal vostro Provider Adsl.

NAT: Impostate **Enable**

Username e Password: Inserite Username e Password forniti dal provider per la connessione alla linea Adsl.

IP address: lasciate 0.0.0.0 per utilizzare l'indirizzo IP dinamico che vi verrà assegnato dal provider al momento della connessione.

Authentication Protocol: selezionate **Chap(Auto)**

Connection: selezionate **Always On**

Idle Timeout (in minutes): impostate 0 per non forzare mai la disconnessione da Internet.

Se la linea è di tipo PPPoE selezionate **PPPoE router** e premete **Next:**

I parametri da impostare sono equivalenti a quelli descritti per la linea PPPoA.
Nel campo **Service name** non inserite nulla, se non espressamente richiesto dal provider.

3.4.3. LINEA RFC 1483 ROUTED CON 1 INDIRIZZO IP STATICO

Le linee con indirizzo IP statico generalmente utilizzano il protocollo RFC 1483 Routed con incapsulamento LLC.

VPI e **VCI:** se non diversamente indicati nel contratto di attivazione della linea Adsl, inserite rispettivamente **8** e **35** come nell'esempio.
NAT: Impostate **Enable**
Encapsulation method: selezionate **LLC Routed**
Selezionate l'opzione **Use the following IP address.**

Inserite in **IP Address** l'indirizzo IP che vi è stato assegnato dal provider.
Inserite in **Netmask** la Subnet Mask che vi è stata indicata dal provider
Inserite in **Gateway** l'indirizzo IP del Gateway che vi è stato assegnato dal provider.

3.4.4. LINEA RFC 1483 ROUTED CON PIÙ INDIRIZZI IP STATICI

La configurazione del router è equivalente a quella per la linea ad un singolo indirizzo IP statico.

Per poter effettivamente utilizzare gli indirizzi IP pubblici che vi sono stati assegnati, dovrete disabilitare il NAT (**NAT: Disable**) e configurare il primo indirizzo IP utile del vostro range sull'interfaccia di LAN del router.

Tutte le macchine che dovranno lavorare con indirizzi IP pubblici dovranno essere configurate nel seguente modo:

IP: uno degli IP pubblici
Subnet Mask: la Subnet associata ai vostri indirizzi pubblici.
Gateway: l'indirizzo pubblico assegnato al router (sulla LAN)
DNS: Gli indirizzi dei DNS forniti dal provider.

3.4.5. DNS

I DNS sono fondamentali per la risoluzione dei nomi, pertanto è necessario che ogni macchina conosca gli indirizzi IP dei DNS.

Se non utilizzate il DHCP server dovete inserire manualmente gli indirizzi dei DNS nelle proprietà della scheda di rete di ogni PC. Avete due opzioni:

1. Inserite nella configurazione dei DNS di ogni PC quelli che vi ha fornito il provider.
2. Inserite nella configurazione dei DNS di ogni PC l'indirizzo IP di LAN del router ed inserite gli indirizzi IP dei DNS forniti dal provider nella finestra di configurazione WAN-DNS del router.

Nel secondo caso, ogni richiesta di risoluzione DNS verrà inviata al router che, grazie alla funzionalità di **DNS Proxy**, è in grado provvedere autonomamente alla risoluzione degli indirizzi.

L'inserimento dei DNS in questa finestra è necessario anche per poter utilizzare correttamente il servizio di **Dynamic DNS.**

3.4.6. ADSL

In questa finestra è possibile definire i parametri fisici della Linea Adsl.

Nel campo **Connect Mode** impostate il tipo di linea Adsl tra le 3 scelte disponibili.

3.5. CONFIGURATION – SYSTEM

Questi menu permettono la configurazione dei parametri di sistema del router.

3.5.1. TIMEZONE

Il router è in grado di regolare automaticamente l'ora, sfruttando i server SNTP pubblici disponibili in Internet.

Time Zone: Enable, abilita il servizio.

Selezionate il fuso orario corretto in **Local Time Zone.**

Daylight Saving: Abilitate questa funzione per gestire automaticamente il passaggio tra ora solare e legale.

3.5.2. REMOTE ACCESS

Premendo **Enable** sarà possibile accedere alla configurazione del router da remoto, collegandosi all'indirizzo IP di WAN del router, per il tempo massimo impostato.
Eseguite un **Logout** prima di chiudere il Browser.
L'accesso è limitato nel tempo, se volete accedere liberamente al router per la configurazione in modo sicuro, create un profilo VPN PPTP per l'accesso alla LAN e quindi alla configurazione del Router.

3.5.3. FIRMWARE UPGRADE

Permette di aggiornare il firmware del dispositivo.

Selezionate **Sfoglia** per indicare il file di aggiornamento ed **Upgrade** per iniziare la procedura.

Non tentare di effettuare un aggiornamento del firmware senza le adeguate istruzioni e i file forniti dal costruttore.

3.5.4. BACKUP/RESTORE

In questa finestra è possibile salvare la configurazione corrente del router per poterla poi ripristinare in un secondo momento.

SALVATAGGIO CONFIGURAZIONE

Premete **Backup**

selezionate **Salva** per salvare il file di configurazione in una cartella sul vostro PC.

RIPRISTINO CONFIGURAZIONE

Premete **Sfoglia** ed indicate il file di configurazione che avete salvato sul PC.
Premete **Restore** per caricare la nuova configurazione.

3.5.5. RESTART ROUTER

Al termine di tutte le configurazione è consigliabile effettuare un "riavvio" del router.
Premete **Restart Router** per riavviare il dispositivo.
Se selezionate la voce **Reset to factory default settings** il router tornerà alla configurazione di fabbrica, **cancellando tutte le impostazioni** e dovrà poi essere riconfigurato.
Dopo un **Reset to factory default settings,** i parametri di accesso alla configurazione saranno:
indirizzo IP: 192.168.1.254
username: admin
password: admin

3.5.6. USER MANAGEMENT

In questa finestra è possibile modificare la password dell'amministratore del router e creare nuovi utenti in grado di accedere alla configurazione.

3.6. CONFIGURATION – FIREWALL

Il Firewall integrato sfrutta le tecniche di stateful packet inspection e packet filtering per fornire due diversi tipi di funzionalità:

1. Firewall: previene gli accessi non autorizzati da internet, con tre livelli di sicurezza:
   - NAT: nasconde gli indirizzi della rete privata LAN all'esterno rendendo difficile l'identificazione di una macchina privata ad un malintenzionato esterno.
   - Firewall Security and Policy: è possibile abilitare o bloccare il passaggio di particolari protocolli in Ingresso.
   - Intrusion Detection: previene o rileva un attacco proveniente dall'esterno.

2. Access Control: previene accessi Internet non autorizzati dalla rete LAN tramite:
   - Firewall Security and Policy: è possibile abilitare o bloccare il passaggio di particolari protocolli in Uscita.
   - MAC Filter rules: abilita o disabilita il passaggio di determinate stazioni in modo univoco (tramite l'indirizzo fisico della scheda di rete)
   - URL Filter: blocca l'accesso ad alcuni siti web, eventualmente in base ad orari prestabiliti.

3.6.1. GENERAL SETTINGS

Security:	Enable, abilita tutte le funzionalità del firewall.
Policy:	Impostate "All blocked/user profile" per creare delle regole personalizzate. In alternativa potete selezionare "Low" o "Medium" o "High" per attivare alcuni profili già preconfigurati.
Block WAN Request:	Se abilitato blocca tutte le richieste in arrivo al firewall da Internet.

Una volta abilitato il firewall, TUTTI i pacchetti in ingresso o uscita verranno bloccati
Sarà necessario impostare delle regole per abilitare il passaggio dei pacchetti desiderati.

La selezione della Firewall Policy influenza solamente la configurazione del menù **Packet Filter**
Per comprendere la creazione delle regole, trovate nell'APPENDICE DEL MANUALE l'elenco delle principali porte utilizzate (l'elenco completo è disponibile alla pagina Internet http://www.iana.org/assignments/port-numbers).

3.6.2. PACKET FILTER

Questa funzione è disponibile solo quando il Firewall è attivo.

Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
hei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	Edit	Delete
hei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
hei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
hei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Block	Edit	Delete
hei_tnet	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Block Block	Edit	Delete
hei_smtp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete

In questa pagina è possibile trovare l'elenco completo delle regole impostate sul dispositivo.

Se nella finestra di configurazione *General Setting* avete impostato un livello di sicurezza preconfigurato in questa finestra troverete già diverse regole (l'elenco completo delle regole per i tre livelli è disponibile nell'appendice).

Per aggiungere nuovi filtri sono disponibili le seguenti funzioni:

Add TCP/UDP filter

Rule Name: Inserite un nome della regola a vostra scelta
Time Schedule: Selezionate il periodo di validità della regola, sempre attiva (Always On), schedulata (TimeSlot1~16), oppure inserita in lista ma disattivata (Disabled)
Source IP Address(es): Impostate l'indirizzo IP di sorgente oppure lasciate 0.0.0.0 (qualsiasi indirizzo)
Destination IP Address(es): Impostate l'indirizzo IP di destinazione oppure lasciate 0.0.0.0 (qualsiasi indirizzo)
Type: Selezionate il protocollo tra TCP, UDP oppure entrambi TCP/UDP
Source Port: Inserite il range di porte sorgenti oppure lasciate 0~65535 (qualsiasi porta)
Destination Port: Inserite il range di porta di destinazione oppure lasciate 0~65535 (qualsiasi porta)
Inbound: *Allow* abilita il passaggio dei pacchetti che corrispondono ai parametri specificati, *Block* ne blocca il passaggio.
Outbound: *Allow* abilita il passaggio dei pacchetti che corrispondono ai parametri specificati, *Block* ne blocca il passaggio.

Selezionate **Apply** per aggiungere la regola.

Add RAW IP filter

Questo filtro offre la possibilità di controllare direttamente un protocollo.
Inserite il numero del protocollo da filtrare in **Protocol Number** e selezionate i permessi in ingresso e uscita.
Selezionate **Apply** per aggiungere la regola.

I principali protocolli sono:

1	ICMP
2	IGMP
4	IP
6	TCP
17	UDP
47	GRE
50	IPSEC ESP
51	IPSEC AH

L'elenco dei protocolli definito dall' RFC 1700 è disponibile nell'APPENDICE DEL MANUALE.

3.6.3. INTRUSION DETECTION

Questa funzione ha lo scopo di proteggere la tua LAN da attacchi esterni, come per esempio attacchi DOS (Denial-of-Service) o port scan.
Lo scopo di questi attacchi è quello di saturare le risorse disponibili sul router e sui server per provocare una temporanea interruzione del funzionamento o in alcuni casi il blocco di tutta la rete LAN.

Il firewall è in grado di riconoscere e di interrompere un tentativo di attacco.
Inoltre è possibile abilitare la funzione di Blacklist, disabilitando per n secondi la ricezione di pacchetti dagli indirizzi IP che sono stati identificati come attaccanti.

Intrusion Detection: selezionate Enable per abilitare le funzioni di Intrusion Detection.
Victim Protection Block Duration: inserite il tempo in secondi, di disconnessione della nostra macchina di LAN, se vittima di un attacco.
Scan Attack Block Duration: questo tempo identifica la durata di permanenza di un indirizzo IP nella Blasklist se ritenuto colpevole di una scansione dei servizi attivi sulla LAN.

DOS Attack Block Duration: questo tempo identifica la durata di permanenza di un indirizzo IP nella Blasklist, quando ritenuto colpevole di un attacco DoS.

Maximum TCP Open Handshaking Count: numero massimo di richieste (SYN) che possono arrivare al router, o ad un server interno, in un secondo; superato questo valore viene abilitata la protezione per evitare il compimento di una attacco SYN flood.

Maximum Ping Count: numero massimo di pacchetti PING che il router può ricevere in un secondo; superata questa soglia il firewall attua le protezioni necessarie a proteggere la LAN da questo tipo di attacco.

Maximum ICMP Count: Inserite il massimo numero di pacchetti ICMP che il router può ricevere in un secondo; superate questa soglia il firewall attua le protezioni necessarie a proteggere la LAN da questo tipo di attacco.

Se siete indecisi sui valori da impostare, non modificate le impostazioni predefinite.

3.6.4. URL FILTER

Questa funzione permette di limitare i siti WEB raggiungibili.

URL Filter

Configuration

URL Filtering	○ Enable ⊙ Disable
Block Mode	Always On
Keywords Filtering	☐ Enable Details
Domains Filtering	☐ Enable Details
	☐ Disable all WEB traffic except for Trusted Domains
Restrict URL Features	☐ Block Java Applet
	☐ Block surfing by IP address

Apply Cancel

Exception List

Name	IP Address

Add

URL Filtering: abilita la funzionalità URL Filter

Block Mode: selezionate la validità delle regole, sempre attiva (Always On), schedulata (TimeSlot1~16), oppure inserita in lista ma disattivata (Disabled).

Keywords Filtering: Se abilitato blocca l'accesso a tutti i siti WEB di cui l'URL contiene una delle stringhe inserite.

Selezionate **Details** per specificare l'elenco delle stringhe da bloccare.

La tabella mostra tutte le stringhe che verranno bloccate, selezionate **Apply** per aggiungerne di nuove oppure **Delete** per rimuovere una parola dalla lista.

Con l'esempio mostrato sopra, ogni sito WEB che contiene nell'URL una delle stringhe in tabella non risulterà accessibile:

www.ludus.it
www.megagames.com
etc. etc.

Il controllo viene effettuato sull'intero URL, pertanto non sarà possibile nemmeno effettuare una ricerca (per esempio da **www.google.it**) che abbia come argomento una delle stringhe impostate. Infatti l'URL che verrà utilizzato per effettuare la ricerca di "giochi" da un qualsiasi motore di ricerca sarà di questo tipo:
http://www.google.it/search?hl=it&ie=UTF-8&oe=UTF-8&q=giochi&btnG=Cerca+con+Google&lr=

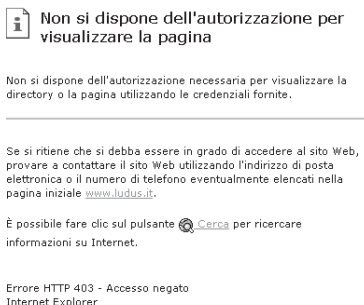
Domains Filtering: Se abilitato applica il filtro basato su domini.

Selezionate **Details** per specificare l'elenco di domini da utilizzare.

La tabella mostra in **Trusted Domain** l'elenco di domini permessi ed in **Forbidden Domain** l'elenco di quelli da bloccare. Selezionate **Apply** per aggiungere nuovi domini oppure **Delete** per cancellarne uno.

Il dominio deve essere scritto come nell'esempio, per www.ferrari.it inserite **ferrari.it** (senza www.)

Se invece di scrivere delle regole per bloccare alcuni siti, preferite indicare gli unici domini raggiungibili, selezionate l'opzione **Disabile all WEB traffic except for Trusted Domains.**
In questo caso sarà possibile raggiungere **solamente** i domini inseriti nella tabella **Trusted Domains.**

Se un PC cerca di raggiungere un sito "bloccato" ottiene solo una pagina di questo tipo:

Block Java Applet: Se selezionata, vengono bloccate tutte le applet java.
Block Surfing by IP Address: Se selezionate blocca l'accesso a pagine web raggiunte senza una richiesta DNS.

3.6.5. FIREWALL LOG

In questa finestra è possibile abilitare o disabilitare i log.

Il log abilitati saranno visibili nel menù **Status – Event Log**

3.7. CONFIGURATION – VPN

Il router supporta delle funzionalità VPN per stabilire connessioni sicure e protette in Internet con altre reti LAN o Client VPN.

Il tunnel VPN può utilizzare il protocollo PPTP oppure il protocollo IPSEC.
Il router riesce a gestire fino a 8 connessioni contemporanee, 4 PPTP e 4 IPSEC.

3.7.1. VPN PPTP (POINT-TO-POINT TUNNELING PROTOCOL)

Questo menu permette la creazione delle policy per il tunneling VPN basato su protocollo PPTP.

Esistono due differenti tipi di connessione PPTP:
Remote Access: permette la connessione alla LAN locale di un singolo client remoto connesso in Internet.
LAN-to-LAN: permette la creazione di un tunnel VPN PPTP tra la LAN locale ed una rete LAN remota.

Enable / Disabile: tramite questa selezione è possibile attivare e disattivare le policy.
Name: Nome mnemonico della policy.
Type: Indica il tipo di policy, Dialin oppure DialOut
Status: indica lo stato attuale della connessione.

Selezionate **Create…** per creare una nuova policy VPN PPTP.

3.7.2. PPTP – REMOTE ACCESS

Connection Name: inserite il nome mnemonico da associare a questa policy, il nome non deve contenere spazi.

Type: **Dial out:** selezionate questo tipo di connessione se volete che sia il router ad attivare la connessione verso un server PPTP remoto raggiungibile in Internet. Nel campo **Server IP Address** inserite l'indirizzo IP del server remoto oppure il suo Hostname.
Dial in: selezionate questa modalità se volete fornire l'accesso alla LAN ad un client remoto connesso in Internet. Nel campo **Private IP Address..** inserite l'indirizzo IP di LAN che volete assegnare al client, una volta connesso.

Username, Password: inserite username e password per il collegamento PPTP.

Auth. Type: selezionate il tipo di autenticazione.

Data Encryption: abilita l'algoritmo di cifratura MPPE. Di default il paramentro è impostato su Auto, quindi negoziato all'instaurarsi della connessione.

Key Lenght: Imposta la lunghezza della Key utilizzata dall'algoritmo MPPE; se lasciato in Auto la Key viene negoziata all'instaurarsi della connessione.

Mode: La Key viene cambiata ogni 256 pacchetti (**stateful)** oppure ad ogni pacchetto (**stateless)**.

Idle time: inserite il tempo di inattività dati per disconnettere il tunnel VPN PPTP; impostando 0 minuti la connessione rimarrà sempre attiva.

Active as Default Route: attiva una default route alla connessione di questa policy.

3.7.3. PPTP – LAN TO LAN

Tutti i parametri sono equivalenti a quelli descritti nella configurazione del Remote Access PPTP.
Peer Network IP / Netmask: identifica la rete LAN remota o una parte della rete remota raggiungibile tramite la connessione PPTP.

Esempio: Per indicare tutta la rete 192.168.2.x inserite:
Peer Network IP: 192.168.2.0
Netmask: 255.255.255.0

3.7.4. VPN IPSEC

Questo menu permette la creazione delle policy per il tunneling VPN basato su protocollo IPSEC.

Selezionate **Create…** per creare una nuova policy.

Connection Name: inserite il nome mnemonico da associare a questa policy, il nome non deve contenere spazi.

Local **NetWork:**
identifica la rete LAN locale o la parte di essa che può utilizzare il tunnel VPN IPSEC.
Single Address: singolo indirizzo IP locale
Subnet: una rete LAN
IP Range: un range d indirizzi IP locali (inizio – fine)

Remote **Secure Gateway Address:**
Indica l’end point, cioè l’indirizzo IP di WAN del router remoto.
NetWork: identifica la rete LAN remota o una parte della rete remota raggiungibile tramite il tunnel VPN IPSEC.
Single Address: singolo indirizzo IP remoto
Subnet: una rete LAN remota
IP Range: un range d indirizzi IP remoti (inizio – fine)

Proposal In questa sezione dovete impostare i vari parametri di crittografia della connessione IPSEC.
Verificate che tutti i paramentri impostati corrispondano esattamente a quelli configurati nel router remoto.

AH Authentication: AH (Authentication Header) specifica l’algoritmo di crittografia da utilizzare per l’header VPN.

ESP: ESP (Encapsulating Security Payload) provvede alla sicurezza dei dati (payload) inviati attraverso il tunnel VPN.
ESP si divide in due parti **Encryption** ed **Authentication** per entrambe è possibile selezionare un algoritmo di crittografia differente.

Perfect Forward Security: se abilitata forza un continuo cambio delle chiavi IPSEC durante la sessione, garantendo che le nuove chiavi non siano in alcun modo in relazione con le precedenti, evitando che dopo aver eventualmente scoperto una chiave, un malintenzionato sia in grado di generarsi tutte le successive.

Pre-Shared Key: inserite la stringa utilizzata come password per generare la crittografia.

Nota: Perfect Forward Security incrementa il grado di sicurezza ma richiede maggior elaborazione dei dati, a discapito delle prestazioni.

3.7.5. ADVANCED OPTIONS

Enable / Disabile: tramite questa selezione è possibile attivare e disattivare le policy.

Cliccate su **Edit** e successivamente sul link **Advanced Options…**

IKE Mode: Selezionate la modalità *Main* oppure *Aggressive.*

IKE Proposal: **Hash Function:** selezionate il tipo di algoritmo da utilizzare.
Encryption: selezionate il tipo di crittografia.
Diffide-Hellman Group: Selezionate una delle modalità disponibili.

Local Id: **Type:**
- **Default**, viene utilizzato l'indirizzo Ip di WAN
- **Domain Name,** viene utilizzato un nome dominio inserito nel corrispondente campo *Content* per presentarsi al server remoto
- **E-mail,** viene utilizzato un indirizzo email inserito nel corrispondente campo *Content* per presentarsi al server remoto

Remote Id: **Type:**
- **Default**, viene utilizzato l'indirizzo Ip di WAN
- **Domain Name,** viene utilizzato un nome dominio inserito nel corrispondente campo *Identifier* per riconoscere il server remoto
- **E-mail,** viene utilizzato un indirizzo email inserito nel corrispondente campo *Identifier* per riconoscere il server remoto

SA life time: Rappresenta il tempo di validità delle chiavi autogenerate.
Phase 1 (IKE): Inserite un valore tra 5 e 15000 minuti, il default è 240.
Phase 2 (IPSec): Inserite un valore tra 5 e 15000 minuti, il default è 60.
Un valore basso di SA aumenta la sicurezza del tunnel ma, ad ogni rinegoziazione delle chiavi il tunnel viene temporaneamente disconnesso.

Ping fo Keepalive: **PING to the IP:** inserite l'indirizzo Ip da pingare per verificare la qualità del tunnel VPN, se l'IP indicato NON risponde il tunnel viene chiuso. Inserendo 0.0.0.0 questa funzione viene disabilitata.
Interval: inserite il numero di secondi tra un test di keepalive ed il seguente. Il valore di default è 10 ma può essere variato tra 1 e 3600 mentre 0 disabilita la funzione.
Disconnection Time after no traffic: chiusura automatica del tunnel VPN a fronte di inattività superiore a x secondi.
Reconnection Time: tempo minimo di attesa prima di rieffettuare una connessione Vpn IPSec. Il tempo minimo è di 3 minuti.

3.7.6. L2TP

Questo menù permette la creazione delle policy per il tunneling VPN basate sul protocollo L2TP.

Esistono due differenti tipi di connessione L2TP:
Remote Access: permette la connessione alla LAN locale di un singolo client remoto connesso in Internet.
LAN-to-LAN: permette la creazione di un tunnel VPN PPTP tra la LAN locale ed una rete LAN remota.

Enable / Disabile: tramite questa selezione è possibile attivare e disattivare le policy.
Name: Nome mnemonico della policy.
Type: Indica il tipo di policy, Dialin oppure DialOut
Status: indica lo stato attuale della connessione.

Selezionate **Create…** per creare una nuova policy VPN L2TP

3.7.7. L2TP - REMOTE ACCESS

Connection Name: inserite il nome mnemonico da associare a questa policy, il nome non deve contenere spazi.

Type: **Dial out:** selezionate questo tipo di connessione se volete che sia il router ad attivare la connessione verso un server L2TP remoto raggiungibile in Internet. Nel campo **Server IP Address** inserite l'indirizzo IP del server remoto oppure il suo Hostname.
Dial in: selezionate questa modalità se volete fornire l'accesso alla LAN ad un client remoto connesso in Internet. Nel campo **Private IP Address..** inserite l'indirizzo IP di LAN che volete assegnare al client, una volta connesso.

Username, Password: inserite username e password per il collegamento L2TP.

Auth. Type: selezionate il tipo di autenticazione.

Idle time: inserite il tempo di inattività dati per disconnettere il tunnel VPN L2TP; impostando 0 minuti la connessione rimarrà sempre attiva.

IP Sec: Se abilitato viene utilizzata la crittografia IPSec.

Authentication: Selezionate l'algoritmo di crittografia per la fase di autenticazione IpSec.

Encryption: Selezionate l'agoritmo di crittografia d utilizzare per i dati

Perfect Forward Secrecy: se abilitata forza un continuo cambio delle chiavi IPSEC durante la sessione, garantendo che le nuove chiavi non siano in alcun modo in relazione con le precedenti, evitando che dopo aver eventualmente scoperto una chiave, un malintenzionato sia in grado di generarsi tutte le successive.

Pre-Shared Key: inserite la stringa utilizzata come password per generare la crittografia.

Per migliorare la sicurezza del tunnel è possibile abilitare anche il parametro Tunnel Authentication.
In questo caso **Remote Host Name** dovrà corrispondere al parametro **Local Host Name** sul router remoto e viceversa.
In **Secret** inserite una password di max 16 caratteri.

3.7.8. L2TP - LAN TO LAN

Tutti i parametri sono equivalenti a quelli descritti nella configurazione del Remote Access L2TP.
Peer Network IP / Netmask: identifica la rete LAN remota o una parte della rete remota raggiungibile tramite la connessione L2TP.

Esempio: Per indicare tutta la rete 192.168.2.x inserite:
Peer Network IP: 192.168.2.0
Netmask: 255.255.255.0

3.8. CONFIGURATION – QOS

La funzione QoS (Quality of Service) permette di migliorare l'allocazione di banda per le applicazioni maggiormente utilizzate.
Le applicazioni VoIp per esempio necessitano di una banda minima per garantire una qualità sufficiente, tramite queste funzioni è possibile garantire un servizio efficiente anche in presenza di altri utilizzi di banda (navigazione, download / upload di grossi file, etc…)

3.8.1. PRIORITIZATION

Tramite questa sezione è possibile aumentare o diminuire la priorità di alcune sessioni nella coda di uscita sulla Wan del router.

Esistono tre livelli di priorità che ripartiscono la banda disponibile:

- **High 60%**
- **Normal 30% (**tutti i pacchetti hanno questa priorità al default**)**
- **Low 10%**

Application: inserite un nome mnemonico per l'applicazione.
Time Schedule: Selezionate il periodo di validità della regola, sempre attiva (Always On), schedulata (TimeSlot1~16), oppure inserita in lista ma disattivata (Disabled)
Priority: Selezionate High o Low per aumentare o diminuire la priorità.
Protocol: Selezionate il tipo di protocollo utilizzato nell'applicazione

Source Port: inserite le porte sorgenti utilizzate dall'applicazione da priorizzare
Destination Port: inserite le porte di destinazione utilizzate dall'applicazione da priorizzare

Source IP Address: inserite il gruppo di indirizzi IP sorgenti utilizzati nell'applicazione da priorizzare
Destination IP Address: inserite il gruppo di indirizzi IP di destinazione utilizzati nell'applicazione da priorizzare

DSCP Marking: imposta anche i parametri di ToS secondo la tabella disponibile nell'appendice.

3.8.2. OUTBOUND IP THROTTLING

Tramite queste impostazioni è possibile definire una BANDA MASSIMA utilizzabile da un'applicazione in uscita LAN -> WAN.

Application: inserite un nome mnemonico per l'applicazione.
Time Schedule: Selezionate il periodo di validità della regola, sempre attiva (Always On), schedulata (TimeSlot1~16), oppure inserita in lista ma disattivata (Disabled)
Protocol: Selezionate il tipo di protocollo utilizzato nell'applicazione
Source Port: inserite le porte sorgenti utilizzate dall'applicazione da priorizzare
Destination Port: inserite le porte di destinazione utilizzate dall'applicazione da priorizzare
Source IP Address: inserite il gruppo di indirizzi IP sorgenti utilizzati nell'applicazione da priorizzare
Destination IP Address: inserite il gruppo di indirizzi IP di destinazione utilizzati nell'applicazione da priorizzare
Upstream Rate Limit: Inserite il limite massimo di banda utilizzabile dall'applicazione, il valore deve essere espresso in moltiplicatori di 32 kbps

3.8.3. INBOUND IP THROTTLING

Tramite queste impostazioni è possibile definire una BANDA MASSIMA utilizzabile da un'applicazione in ingresso WAN -> LAN.

Application: inserite un nome mnemonico per l'applicazione.
Time Schedule: Selezionate il periodo di validità della regola, sempre attiva (Always On), schedulata (TimeSlot1~16), oppure inserita in lista ma disattivata (Disabled)
Protocol: Selezionate il tipo di protocollo utilizzato nell'applicazione
Source Port: inserite le porte sorgenti utilizzate dall'applicazione da priorizzare
Destination Port: inserite le porte di destinazione utilizzate dall'applicazione da priorizzare
Source IP Address: inserite il gruppo di indirizzi IP sorgenti utilizzati nell'applicazione da priorizzare
Destination IP Address: inserite il gruppo di indirizzi IP di destinazione utilizzati nell'applicazione da priorizzare
Upstream Rate Limit: Inserite il limite massimo di banda utilizzabile dall'applicazione, il valore deve essere espresso in moltiplicatori di 32 kbps

3.9. CONFIGURATION – VIRTUAL SERVER

La funzione **Virtual Server** permette l'accesso a Server e servizi presenti nella LAN locale, da parte di utenti remoti connessi in Internet.
I servizi selezionati verranno resi disponibili sull'indirizzo IP di WAN del router.

Normalmente questi Server NON sono raggiungibili da Internet perché:

1. Il Server ha un indirizzo IP privato
2. Il protocollo NAT nasconde la LAN interna.

In questa finestra è possibile configurare tre differenti tipi di Virtual Server:

Add Virtual Server: permette l'inserimento di un singolo Virtual Server.

Edit DMZ Host: permette di definire un virtual server esteso, tutte le porte NON inserite in altre regole di Virtual Server verranno indirizzate sull'indirizzo IP inserito nella funzione DMZ (De-militarized Zone). Il nome di questa sezione indica che la zona è NON controllata pertanto la macchina con indirizzo IP DMZ non è protetta dal firewall.

Edit One-to-One NAT: permette la definizione di un gruppo di indirizzi IP aggiuntivi sulla WAN, tali indirizzi IP possono quindi essere associati ad altrettanti indirizzi IP privati interni alla LAN (ex. Server Web e Server di posta).

3.9.1. ADD VIRTUAL SERVER

Time Schedule: Selezionate il periodo di validità della regola, sempre attiva (Always On), schedulata (TimeSlot1~16), oppure inserita in lista ma disattivata (Disabled)

Application: Inserite il nome mnemonico dell'applicazione che la regola andrà a gestire, ciccando sul link **Helper** è possibile selezionare uno dei protocollo più comunemente utilizzati per effettuare una rapida configurazione.

Protocol: selezionate il tipo di protocollo.

External Port: Selezionate il range di porte che l'applicazione utilizza.

Redirect Port: Inserite il range di porte che verranno utilizzate dall'Ip privato per gestire l'applicazione. (solitamente External Port e Redirect Port sono uguali).

Internal IP Address: inserite qui l'indirizzo IP della macchina che utilizza l'applicazione configurata. Cliccate il link **Candidates** per visualizzare l'elenco delle macchine collegate in rete (già scoperte dal dispositivo).

3.9.2. EDIT DMZ HOST

Selezionate **Enable** per attivare questa funzionalità.

Internal IP Address: inserite qui l'indirizzo IP della macchina che verrà posta in “DMZ”. Cliccate il link **Candidates** per visualizzare l'elenco delle macchine collegate in rete (già scoperte dal dispositivo).

3.9.3. EDIT ONE-TO-ONE NAT

Se il vostro abbonamento Adsl prevede l'utilizzo di più indirizzi IP aggiuntivi potete mantenere la navigazione delle macchine tramite NAT, mentre i vostri Server potranno essere raggiungibili da Internet sfruttando i vostri indirizzi Pubblici.

NAT Type: Selezionate il tipo di NAT desiderato. La posizione di Default **Disabile** disabilita la funzione **One-to-One NAT.**

Global IP Address:
- **Subnet:** la subnet degli indirizzi IP aggiuntivi viene solitamente indicata dal vostro provider. In caso contrario utilizzate il metodo seguente.
- **IP Range:** inserite il Range di indirizzi IP inserendo l'indirizzo IP di inizio e di fine del gruppo.

Per configurare un associazione 1 ad 1 cliccate sul link **Add Entry**->

Time Schedule: Selezionate il periodo di validità della regola, sempre attiva (Always On), schedulata (TimeSlot1~16), oppure inserita in lista ma disattivata (Disabled)

Application: Inserite il nome mnemonico dell'applicazione che la regola andrà a gestire, ciccando sul link **Helper** è possibile selezionare uno dei protocollo più comunemente utilizzati per effettuare una rapida configurazione.

Protocol: selezionate il tipo di protocollo.

Global IP: Inserite l'indirizzo aggiuntivo da utilizzare in quest'applicazione.

External Port: Selezionate il range di porte che l'applicazione utilizza.

Redirect Port: Inserite il range di porte che verranno utilizzate dall'Ip privato per gestire l'applicazione. (solitamente External Port e Redirect Port sono uguali).

Internal IP Address: inserite qui l'indirizzo IP della macchina che utilizza l'applicazione configurata. Cliccate il link **Candidates** per visualizzare l'elenco delle macchine collegate in rete (già scoperte dal dispositivo).

3.10. CONFIGURATION – TIME SCHEDULE

Tutte le funzione principali del router possono avere validità in base ai giorni / orari della settimana, è possibile creare fino a 16 differenti gruppi di giorni e orari.

Time Schedule

Time Slot

ID	Name	Day in a week	Start Time	End Time		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Edit	Clear
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Edit	Clear
3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	Edit	Clear
4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	Edit	Clear
5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	Edit	Clear

In questa finestra viene mostrato un riepilogo dei gruppi configurati, al default tutti i 16 gruppi sono configurati in questo modo:

dal Lunedì (Monday) al Venerdì (Friday) e dalle 08:00 alle 18:00.

Day in a week: la settimana parte domenica (sunday) e termina sabato (saturday), l'inziale del giorni con lettere maiuscola indica che il giorno è compreso nel gruppo.

Cliccate sul link **Edit** per modificare uno dei 16 slot.

Name: inserite il nome mnemonico del gruppo che volete creare.

Day: selezionate i giorni di validità della regola

Start Time / End Time: inserite gli orari di vanità della regola, da Start ad End.

3.11. CONFIGURATION – ADVANCED

Questo menu permette di impostare alcuni parametri e funzioni avanzate.

3.11.1. STATIC ROUTE

Se Michelangelo Office Pro V non è l'unico router presente nella rete LAN potrebbe essere necessario creare delle route statiche (regole di instradamento) per indirizzare i pacchetti verso le altre reti (e altri Gateway).

3.11.2. DYNAMIC DNS

La maggior parte degli abbonamenti Adsl utilizzano un indirizzo IP dinamico, pertanto l'indirizzo di WAN del router può cambiare ad ogni connessione.
Per risolvere questo problema sono disponibili in Internet dei servizi denominati **Dynamic DNS (DDNS).**
Questi servizi DDNS permettono di associare un nome di dominio ad un indirizzo IP in modo dinamico, dopo aver effettuato una registrazione gratuita oppure a pagamento.

Dynamic DNS: Selezionate Enable per abilitare il servizio.
Selezionate il vostro server del servizio da **Dynamic DNS** ed inserite i dati del vostro account.
In **Period** selezionate ogni quanti giorni volete effettuare un aggiornamento dell'indirizzo.

Ogni qualvolta il router rileva un nuovo indirizzo IP sulla WAN, effettua automaticamente una nuova registrazione al server DDNS (nell'esempio **www.dyndns.org**) impostato, aggiornando così l'indirizzo IP di WAN corrente.
Un host, o altro router, che da internet faccia riferimento al dominio attivato, otterrà come risultato l'indirizzo IP attuale, e potrà così raggiungere i servizi eventualmente messi a disposizione sulla porta WAN (tramite Virtual Server).

3.11.3. CHECK EMAILS

Michelangelo Office Pro V è in grado di controllare periodicamente un account di posta e di indicare con l'apposito led sul frontale la presenza di e-mail nella casella di posta.

3.11.4. DEVICE MANAGEMENT

In questa finestra è possibile modificare le proprietà del Web Server interno per la configurazione dell'hardware.

Host Name: Inserite l'Host name da associare al router.

HTTP Port: permette la modifica della porta sulla quale è attivo il Web Server. Se modificate la porta, inserite un valore **superiore a 1024.**
Per entrare in configurazione del router è quindi necessario collegarsi alla porta scelta; se impostate la porta 8080, nel browser dovrete scrivere **http://192.168.1.254:8080.**
Selezionate sempre la porta 80 (HTTP) oppure in alternativa una porta superiore a 1024.

Management IP Address: lasciate impostato 0.0.0.0 se volete permettere la configurazione del router da un qualsiasi indirizzo IP di LAN.
In alternativa potete limitare l'accesso alla configurazione ad un solo indirizzo IP, inserendone il valore .

Expire to auto-logout: nella configurazione del dispositivo può accedere un solo utente alla volta.
Se l'utente non effettua il logout, cliccando sull'apposito pulsante, mantiene impegnata la sessione di configurazione impedendo l'accesso ad altri utenti. Per ovviare a questo problema è possibile impostare un logout automatico allo scadere di n secondi di inattività.

Universal Plug and Play (UPnP)
UPnP: Abilitate la configurazione tramite il protocollo UPnP selezionando Enable sulla porta **UPnP Port**.

SNMP Access Control Michelangelo Office Pro V supporta il protocollo SNMP.
E' possibile configurare la password di accesso alle tre Community e l'indirizzo IP abilitato ad accedere (0.0.0.0 per permettere l'accesso da tutti gli indirizzi).
Al default la password per la **Read Community** è **public**, per la **Write Community** è **password** e la **Trap Community** è disabilitata.

3.11.5. IGMP

IGMP Forwardin: Se abilitato permette la gestione dei pacchetti Multicast.

IGMP Snooping: Se abilitato permette allo switch di bloccare l'invio dei pacchetti multicast sulle porte ove non ne rileva un utilizzo.

3.12. STATUS

Il menù **Status** mostra un riepilogo della configurazione del router.
In particolare:
Software Version è la versione Firmware caricata nel dispositivo
LAN e WAN riepilogano le configurazioni di LAN e WAN.

3.12.1. STATUS – ARP TABLE

In questa finestra è possibile controllare gli indirizzi IP e i MAC Address di tutte le macchine che sono entrate in contatto con il Router.

3.12.2. STATUS – DHCP TABLE

Questa finestra mostra tutti gli indirizzi IP che sono stati assegnati via DHCP Server in associazione al MAC Address e al nome della scheda di rete che ha richiesto l'indirizzo.
Expiry rappresenta il tempo di validità dell'indirizzo.

3.12.3. STATUS – PPTP STATUS, IPSEC STATUS, L2TP STATUS

Questa due finestre mostrano un riassunto delle eventuali connessioni PPTP o IPSEC configurate e ne visualizzano lo stato.

3.12.4. STATUS – EMAIL STATUS

In questa finestra è possibile verificare il numero di Email che il router ha rilevato sulla casella di posta da controllare.
Reset Status: azzera il contatore (e quindi spegne anche il led MAIL)
Check Now ! forza un controllo del numero di Email nella casella di posta configurata.

3.12.5. STATUS – EVENT LOG, ERROR LOG

Queste finestra mostrano i Log di sistema.

Se abilitate i log nella configurazione del firewall, verranno tutti riportati nella pagina **Event Log.**

A. APPENDICE

A.1. PORTE TCP/UDP MAGGIORMENTE UTILIZZATE

Nome	Numero	Descrizione
ftp-data	20/tcp	File Transfer (Default Data)
ftp-data	20/udp	File Transfer (Default Data)
ftp	21/tcp	File Transfer (Control)
ftp	21/udp	File Transfer (Control)
ssh	22/tcp	SSH Remote Login Protocol
ssh	22/udp	SSH Remote Login Protocol
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
smtp	25/tcp	Simple Mail Transfer
smtp	25/udp	Simple Mail Transfer
domain	53/tcp	Domain Name Server
domain	53/udp	Domain Name Server
http	80/tcp	World Wide Web HTTP
http	80/udp	World Wide Web HTTP
www	80/tcp	World Wide Web HTTP
www	80/udp	World Wide Web HTTP
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP
pop3	110/tcp	Post Office Protocol - Version 3
pop3	110/udp	Post Office Protocol - Version 3
nntp	119/tcp	Network News Transfer Protocol
nntp	119/udp	Network News Transfer Protocol
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
snmp	161/tcp	SNMP
snmp	161/udp	SNMP
snmptrap	162/tcp	SNMPTRAP
snmptrap	162/udp	SNMPTRAP
pptp	1723/tcp	pptp
pptp	1723/udp	pptp
ms-wbt-server	3389/tcp	
ms-wbt-server	3389/udp	MS WBTerminal Server

A.2. PACKET FILTER – DEFAULT CONFIGURATION

Applicazione	Protocollo	Porta n°		Firewall - High		Firewall - Medium		Firewall - Low	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS	UDP(17)	53	53	NO	YES	NO	YES	YES	YES
DNS	TCP(6)	53	53	NO	YES	NO	YES	YES	YES
FTP	TCP(6)	21	21	NO	NO	NO	YES	NO	YES
Telnet	TCP(6)	23	23	NO	NO	NO	YES	NO	YES
SMTP	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS	TCP(6)	119	119	NO	NO	NO	YES	NO	YES
Real Audio / Real Video	UDP(17)	7070	7070	NO	NO	YES	YES	YES	YES
PING	ICMP(1)			NO		NO	YES	NO	YES
H.323	TCP(6)	1720	1720	NO	NO	NO	YES	YES	YES
T.120	TCP(6)	1503	1503	NO	NO	NO	YES	YES	YES
SSH	TCP(6)	22	22	NO	NO	NO	YES	YES	YES
NTP	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTPS	TCP(6)	443	443	NO	NO	NO	YES	NO	YES
ICQ	TCP(6)	5190	5190	NO	NO	NO	NO	YES	YES

A.3. TOS BIT CONFIGURATION

Router	DSCP Mapping Table Standard DSCP	ToS Bit
Disabled	None	No ToS
Best Effort	Best Effort	000000
Premium	Express Forwarding	101110
Gold service (L)	Class 1, Gold	001010
Gold service (M)	Class 1, Silver	001100
Gold service (H)	Class 1, Bronze	001110
Silver service (L)	Class 2, Gold	010010
Silver service (M)	Class 2, Silver	010100
Silver service (H)	Class 2, Bronze	010110
Bronze service (L)	Class 3, Gold	011010
Bronze service (M)	Class 3, Silver	011100
Bronze service (H)	Class 3, Bronze	011110

A.4. ELENCO SERVER DNS

Gli indirizzi riportati in questa pagina hanno lo scopo di aiutare nella configurazione del router, qualora questi dati non siano stati specificati dal provider.
La gestione di questi indirizzi dipende solo dai rispettivi provider, pertanto non è possibile garantirne la funzionalità nel tempo.

TIN

dns1.village.tin.it	195.14.96.135
dnsca2.tin.it	212.216.172.222
dnscache2.tin.it	212.216.172.162
dns2.tin.it	194.243.154.51
dnscache1.tin.it	212.216.172.62
dns1.fullcompany.telecomitalia.it	212.131.30.42
dnsca.tin.it	212.216.112.112
dnsca.tin.it	195.31.190.31
dns.tin.it	194.243.154.62

Interbusiness

r-dns.interbusiness.it	151.99.125.1
dns2.interbusiness.it	151.99.125.3
dns.interbusiness.it	151.99.125.2
server-b.cs.interbusiness.it	151.99.250.2

Infostrada

ns2.libero.it	193.70.192.100
ns1.libero.it	195.210.91.100
cns-a.libero.it	193.70.192.25
cns-b.libero.it	193.70.152.25

Wind

dns.wind.it	212.245.255.2
dns2.wind.it	212.245.158.66
dns.inwind.it	212.141.53.123
dns2.wind.it	212.245.158.66

Atlanet

ns1.atlanet.it	213.234.128.211
ns2.atlanet.it	213.234.132.130
ns1.its.it	151.92.2.35
ns.telexis.it	213.199.1.132

McLink

dns.mclink.it	195.110.128.1

Flashnet

dns.flashnet.it	194.247.160.1
dns2.flashnet.it	194.247.160.8

Albacom

ns2.albacom.net	212.17.192.209

I.Net

urano.inet.it	194.20.8.1
venere.inet.it	194.20.8.4

Elitel

elitel.it	212.34.224.193
ns.elitel.it	212.34.224.132
ns2.elitel.it	217.146.65.7
ns3.elitel.it	217.146.65.80

Tiscali

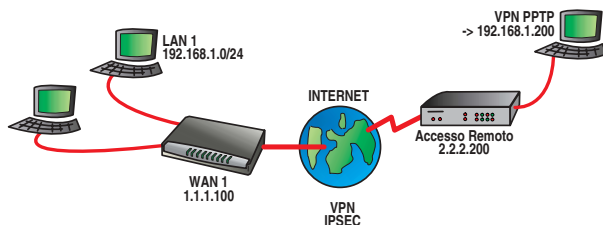
ns.tiscali.it	195.130.224.18
sns.tiscali.it	195.130.225.129

Jumpy

-	212.17.192.216
-	212.17.192.56

Public DNS

dns.nic.it	193.205.245.5
dns2.nic.it	193.205.245.8
nameserver.cnr.it	194.119.192.34

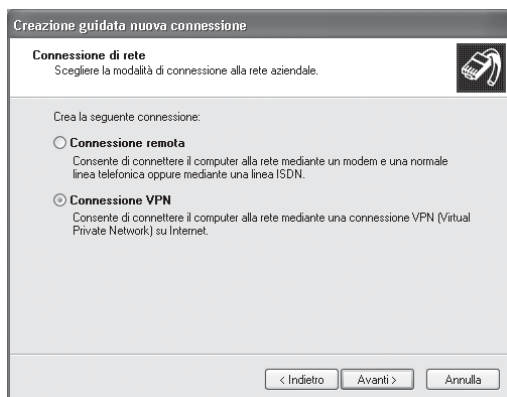
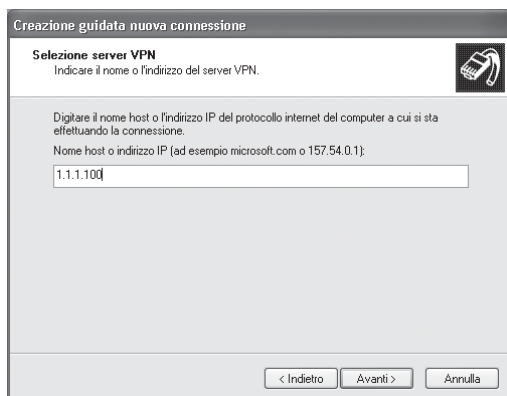
A.5. ACCESSO DA REMOTO CON VPN PPTP

Da una qualsiasi postazione remota connessa in Internet, è possibile accedere alla rete locale LAN1 utilizzando la connessione VPN PPTP fornita da Windows®.

Michelangelo Office Pro V deve essere configurato nel seguente modo:

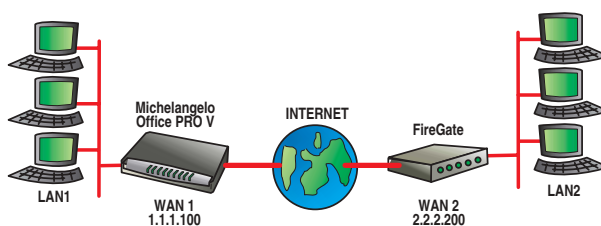
Con questa configurazione si abilita un host remoto ad accedere direttamente alla nostra LAN, l'host remoto riceverà un indirizzo IP da noi specificato (in questo caso 192.168.1.200).

La configurazione di windows deve essere effettuata nel seguente modo.

Create una **Connessione alla rete aziendale**

Selezionate il tipo **Connessione VPN**

Inserite l'indirizzo IP di WAN del router Michelangelo Office Pro V .

Attivate la vostra connessione Internet classica e eseguite la connessione appena creata:

Al termine della connessione, potrete accedere a tutte le risorse disponibili nella rete LAN 1.

A.6. CONNESSIONE IPSEC PRO-V E FIREGATE

In questo esempio viene creato un tunnel VPN tra una rete LAN 1 ed una rete LAN 2 attraverso Internet, utilizzando la crittografia IPSEC.
La rete LAN 1 utilizza un Router **Michelangelo Office Pro-V ADSL2+**.
La rete LAN 2 utilizza un dispositivo VPN in grado di gestire le connessioni IPSEC con Pre-Shared Key, come il Firewall **Firegate 10C.**

La configurazione del Michelangelo è la seguente:

Il tunnel VPN realizzato permette il passaggio di pacchetti dalla LAN 1 alla LAN 2, pertanto:

Local Network: tutta la *Subnet* con Ip Address 192.168.1.0 con Netmask 255.255.255.0, cioè tutti gli indirizzi compresi tra 192.168.1.1 e 192.168.1.254

Remote Network: tutta la *Subnet* con Ip Address 192.168.0.0 con Netmask 255.255.255.0, cioè tutti gli indirizzi compresi tra 192.168.0.1 e 192.168.0.254

L'indirizzo di **Secure Gateway Address** è 2.2.2.200 cioè l'indirizzo pubblico assegnato alla WAN del Firegate 10C.
Per la protezione dei pacchetti viene impostato **ESP.**
Autenticazione crittografata con algoritmo **MD5.**
Pacchetti crittografati con algoritmo **DES.**

Pre-shared Key: una password a nostra scelta (uguale in entrambi i dispositivi).

Dopo aver applicato la configurazione cliccando su ***Apply*** disabilitate la Vpn creata per poterla editare.
Cliccando sul link ***Advanced Options*** si accede alla successiva pagina di configurazione:

La configurazione del **Firegate 10C** è la seguente:

VPN Policy Definition

Name: MichPROv ☑ Enable Policy
☐ Allow NetBIOS traffic

Remote VPN endpoint ○ Dynamic IP
◉ Fixed IP: 1 . 1 . 1 . 100
○ Domain Name:

Local IP addresses
Type: Subnet address IP address: 192 . 168 . 0 . 0 ~ 0
Subnet Mask: 255 . 255 . 255 . 0

Remote IP addresses
Type: Subnet address IP address: 192 . 168 . 1 . 0 ~ 0
Subnet Mask: 255 . 255 . 255 . 0

Authentication & Encryption
☐ AH Authentication MD5
☑ ESP Encryption DES Key Size: n/a (AES only)
☑ ESP Authentication MD5

Remote VPN EndPoint è l'indirizzo 1.1.1.100, cioè l'indirizzo IP pubblico assegnato alla WAN del Michelangelo Office Pro-V ADSL2.
Le rete locale e remota vengono definite sulla base della subnet come nella configurazione precedente.
La crittografia è impostata per utilizzare gli stessi algoritmi impostato sul Michelangelo.
Firegate 10C offre la possibilità di impostare dei parametri aggiuntivi che verranno comunque negoziati in automatico con il Michelangelo.

Nel caso in cui utilizzate il Michelangelo Office PRO-V ADSL2 con il firewall attivo, è necessario aprire, tramite il menù Packet Filter la porta 500 in UDP e il protocollo RAW IP 50.